REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-6 and 13-24 stand rejected under 35 U.S.C. §103(a) over *Ko* (US 7,024,694) in view of *Moran* (6,647,400). In response, claims 1 and 14 are amended, and as presented below, are believed to be patentable over the applied art for the failure of the applied art to disclose, teach or suggest all of Applicants' recited claim features.

As amended, independent claim 1 recites, inter alia, a method of detecting critical file changes, comprising, *inter alia*, "generating a read request for an event representing at least one system call, wherein the event is a kernel audit record removed from a buffer of an intrusion detection data source (IDDS)." Support for the amendments is provided by US Patent No. 7,099,866, entitled "METHOD OF GENERATING AND PRESENTING KERNEL DATA," incorporated by reference in its entirety in Applicants' specification. Specifically, column 8, lines 23-25 discloses wherein "pseudo-driver 310 reads the contents from the circular buffer 340 in response to a user issued read to the driver 310. Neither *Ko* nor *Moran* discloses, teaches, or suggests at least this feature.

Applicants respectfully submit that at the Examiner cited passages at column 5, lines 20-24 and 41-43, *Ko* appears to only disclose examining an audit log for intrusion detection purposes. Furthermore, the flowchart of *Ko*'s Fig. 4 only discloses producing an audit log (410) and examining the audit log (412). Applicants respectfully submit that neither *Ko* nor *Moran* teach or disclose the claimed "generating a read request for an event representing at least one system call, wherein the event is a kernel audit record removed from a buffer of an intrusion detection data source (IDDS)." (Emphasis added). For at least this reason, withdrawal of the rejection is respectfully requested.

Claim 1 further recites:

> "routing the event to a template, the event comprising multiple parameters and the template comprising a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node."

The Examiner asserts that *Ko*, at column 4, lines 45-60, discloses this feature. Applicants respectfully disagree. At the cited text, *Ko* appears to only disclose recording a target attribute if

a specific auditing criterion is satisfied. Nowhere does *Ko* disclose, teach, or suggest a template comprising a sequence of connected logic nodes, let alone logic nodes comprising at least one input node, at least one filter node, and at least one output node, as recited in claim 1.

The PTO further posits that *Ko*, at column 5, lines 29-46, discloses "filtering the event, based on the sequence of logic nodes of the template" (emphasis added), as recited in claim 1. Applicants respectfully disagree. At the cited passage *Ko* appears to only disclose wherein "producing audit log 105 can involve filtering the target attribute to reduce an amount of data stored in audit log 105." (Emphasis added). Applicants submit that claim 1 is distinguished from *Ko* on at least two counts. First, unlike Applicants method that filters events read from the IDDS, *Ko* appears to filter data prior to being logged and it is the output of the filtering that is stored. Second, as previously presented, whereas Applicants' filtering method is based on the sequence of logic nodes of the template, the filtering done by *Ko* appears to involve determining a characteristic of the target attribute in order to reduce an amount of data stored. Applicants respectfully submit, therefore, that the filtering performed by the Applicants is distinguished from the filtering of *Ko*. For at least this reason, withdrawal of the rejection is respectfully requested.

Based on at least the foregoing reasons, the combination of *Ko* and *Moran* fails to disclose, teach or suggest each limitation recited in amended claim 1. Therefore, the method of claim 1 is patentable over *Ko* and *Moran*, and the rejection is respectfully requested to be withdrawn.

System claim 14 is amended similar to claim 1, and is likewise patentable over *Ko* and *Moran*. Claims 2-6, 13, and 15-24 depend, either directly or indirectly, from claims 1 and 14, include further features, and are patentable over the asserted combination of references for at least the reasons advanced above with respect to claim 1.

Conclusion

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claim 1-6 and 13-24 are earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

Mark Crosbie *et al.*

Randy A. Noranbrock
Registration No. 42,940
Telephone: (703) 684-1111

HEWLETT-PACKARD COMPANY
IP Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80528-9599
Telephone: (970) 898-7057
Facsimile: 281-926-7212
Date: **April 23, 2008**
RAN/ERM/bjs